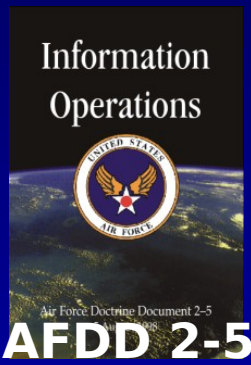
College of Aerospace Doctrine, Research, and Education

Security Measures IW-130

Overview

- Operation Security (OPSEC)
- Information Conditions (INFOCON)
- Information Assurance (IA)

Operations Security (OPSEC)



AFDD 2-5

… a process of identifying critical information and subsequently analyzing the friendly actions that accompany military operations and other activities to:

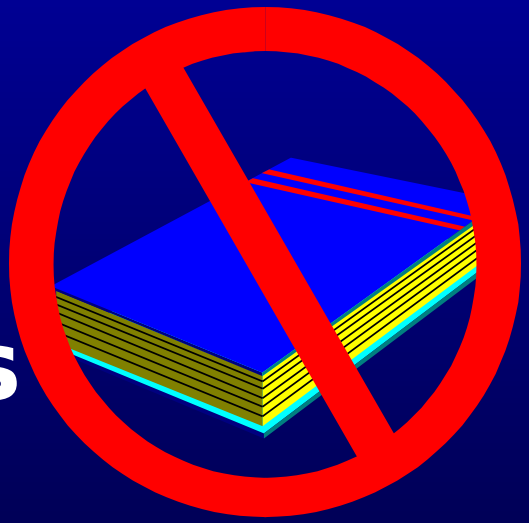
- **Identify actions that can be observed by adversary systems**
- **Determine indicators that could be interpreted or pieced together to derive critical information**
- **Select and execute measures that eliminate or reduce the vulnerabilities of friendly actions**

Unique Characteristic

OPSEC is a PROCESS

1 2 3 4 5

OPSEC is NOT a set of Rules



The Differences

Traditional Security	OPSEC
Most information is classified	Usually unclassified
Addresses the general threat	Addresses specific adversarie
Risk applies to all situations	Risk decisions are event spec
Directed by security regulations	Directed by operational CC
Countermeasures established	Countermeasures often uniqu
Concealment only	Eliminates, conceals, disguises, or deceives

Five Step OPSEC Process

1. Identify Critical Information
2. Determine Threat
3. Analyze Vulnerabilities
4. Assess Risk
5. Apply appropriate OPSEC Measures

1 2 3 4 5

Identify Critical Info

- **Identify the questions the adversary will ask …**
  - **Where do I get the information?**
  - **Who has the information?**
  - **When do I need the information?**
  - **How do they transfer the information?**
  - **How is the information protected?**

Essential Elements of Friendly Information (

Critical Info Examples

- Diplomatic Negotiations
  - Military capabilites / Intelligence capabilities
- Military Intervention
  - Intentions / Capabilities / Constraints
  - Targets / Timing / Logistics / Limitations
- Counter-terrorism
  - Forces / Staging locations / Ingress-Egress Methods
- Mobilization
  - Alert posture / Impact on civil economy / transpo
- ISR
  - Purpose / Targets / Timing / Process capabilities

1 2 3 4 5

Determine Threat

- Who is the adversary?
- What are the adversary's goals?
- What is the adversary's opposition strategy?
- What critical information is already known?
- What are the adversary's collection capabilities?

1 2 3 4 5

Analyze Vulnerabilities

Indicators &
+ Actions

= Collection Vulnerability

Indicators

Signature: Uncommon or unique features

Associations: Specific support equipment

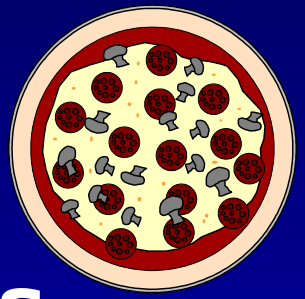
Profiles: Unit missions (Homepage)

Contrasts: Non-standard activities

Exposure: Observation Time

Actions

Pizza Delivery



DV Suites

Intramural Sports

E-Mail Reply / Router

BX Supplies

Government Credit Card

STU-III Usage

Collection

Overt and Clandestin

Federation of American Scientists

Open Source Intelligence (OSINT)

Human Intelligence (HUMINT)

SPOT IMAGE

hagery Intelligence (IMINT)

Signals Intelligence (SIGINT)

Communications Intelligence

Intelligence

SPACE IMAGING

trumentation Signals

Technical Intelligence (TECHINT)

CNN networks
Today on CNN

Indicators & Actions + Collection

Signature: Uncommon or unique features

Associations: Specific support equipment

Profiles: Unit missions

Contrasts: Not standard

Exposu

Open Source Intelligence (OSINT)

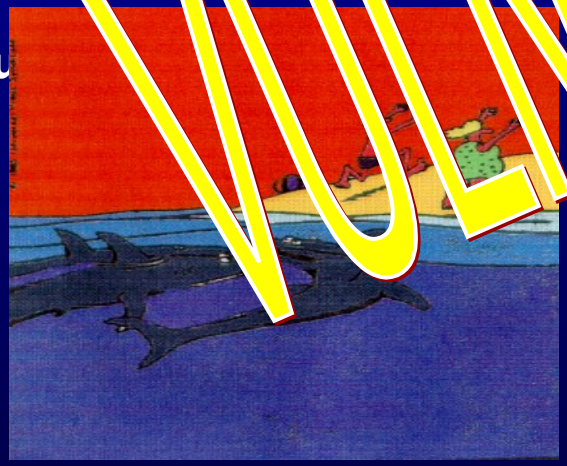
Human Intelligence (HUMINT)

Imagery Intelligence (IMINT)

Signals Intelligence (SIGINT)

Technical Intelligence (TECHINT)

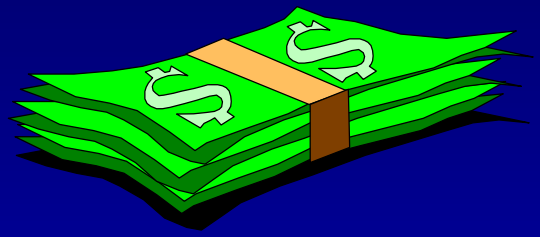
VULNERABILITY



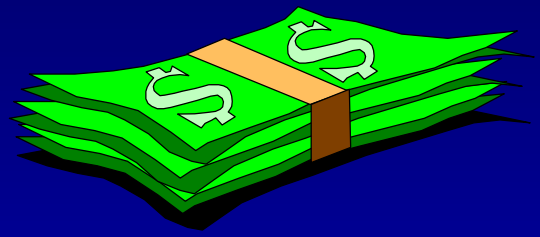
SPACE IMAGING

1 2 3 **4** 5

Assess Risk



Cost



vs

Potential Harmful Effects

The Cost Can Be High

1 2 3 4 **5**

Apply OPSEC Measures

- **Prevent the adversary from detecting an indicator**
- **Provide an alternative analysis of an indicator**
- **Attack or deny the adversary's collection system**
- **Integrate OPSEC with other IO elements**

“Full Victory - Nothing Else”

Gen. Dwight D. Eisenhower

Five Step OPSEC Process

1. Identify Critical Information
2. Determine Threat
3. Analyze Vulnerabilities
4. Assess Risk
5. Apply appropriate OPSEC Measures

OPSEC Concerns

- 25 Feb - 8 Mar 02 - Human Intelligence Vulnerability Assessment (HVA) at “X”AFB
- “X”AFB in Force Protection Condition BRAVO
- Simulated Foreign Intel Security Service threat = 4 AFOSI Team Members (TMs)
- Emulated 4 typical collection methods:
  - visual observations
  - trash covers
  - pretext conversations (telephone & face-to-face)
  - open source literature searches

Visual Observations

- People bused to “X”AFB, no variances in time
- Daytime installation access with only a DoD vehicle decal
- Unsecured installation facilities:
  - Recycling Center gate and facility
  - XXX Center front door. TMs obtained access to over 2700 personnel files.
  - MPF window
  - Mechanical room
  - Fire escape
  - Exposed Cat 5 computer lines
  - Found a logged on computer terminal with admin privileges (later exploited)

Trash Covers

- Active duty military ID card request letter from a trash receptacle. Letter was for lost ID card and was signed by commander.
- On 3 separate occasions, TMs gained access to XAFB recycling facility through an unsecured gate. An unsecured outer window provided access to office and storage areas. Once inside, TMs located a large recycling receptacle that contained thousands of privacy act and FOUO documents. TMs also noted 2 unsecured government vehicles at the facility. TMs obtained the following from the recycling facility:

Trash Covers

- Flight maps and flight approach procedure publications
- Unit personnel phone directory, org chart, recall and flight rosters
- Completed and signed National Security Questionnaires (SF 86)
- Copy of an active duty military ID card and 2 social security cards
- Completed and signed travel voucher
- Boeing Operational Flight Trainer Study Guide for F-16s
- Aircraft Operational Status Chart
- List of incoming personnel
- Graduation roster
- Department of the AF letterhead
- FOUO email
- Shipping lists for personnel departing “X”AFB
- Copy of orders in support of exercise Operation XXX and info about 3 people who were to support the Operation
- Copy of two credit card receipts

Trash Covers

- On 3 separate occasions, TMs gained access to MPF through an unsecured outer window. TMs found personnel records, Unfavorable Information Files (UIF), and orders. TMs conducted a trash cover at 2300. An active duty AF member approached the two TMs and stated, “What’s up” and proceeded to another office area.

Pretext Conversations

- Obtained a “X”AFB telephone directory from billeting employee
- An active duty person stated “X”AFB provides a high volume of troops in support of current overseas operations
- Contacted MPF employee to obtain the birth date of the person who had lost his ID card. MPF employee provide the date
- SFS member stated he was tasked for the next deployment rotation; SFS manpower on “X”AFB was reduced from 109 to 84 people

Pretext Conversations

- TM contacted the “X”AFB Deployment Processing Unit (DPU) and posed as a Captain from AFPC readiness. TM requested the current and projected number of “X”AFB’s personnel deployed in support of Operations XXX and XXXX. TM was informed that 184 personnel were deployed and 113 personnel were projected to deploy. TM asked for a hard copy of the report and stated he would send a Lt to DPU to obtain the info. TM arrived in uniform and obtained the info. The documents included names, ranks, SSN, AFSCs, depart and return dates, and locations were personnel were deployed -- info was labeled FOUO.

Open Source Literature Searches

- Only provided XX graduation / visitation procedures and general info about the X Wing and its organizations

Information Operations Condition (INFOCON)

- … presents a structured, coordinated approach to defend against and react to adversarial attack on DoD computer and telecommunication networks and systems
- … based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent
- … established by the Secretary of Defense; administered through the Commander JTF-CND

INFOCON Level: NORMAL
Normal Activity

CRITERIA	RECOMMENDED ACTIONS
No significant activity.	- Ensure all mission critical info and info systems (including applications and databases) and their operational importance are identified. - Ensure all points of access and their operational necessity are identified. - On a continuing basis, conduct normal security practices. For example: -- Conduct education and training for users, admin, & management -- Ensure effective password mgmt program is in place -- Conduct periodic internal security review and external vulnerability assessments. -- Conduct normal auditing, review,

INFOCON Level: ALPHA
Increased Risk of Attack

CRITERIA	RECOMMENDED ACTIONS
- Indications & Warning (I&W) indicate general threat. - Regional events occurring which affect US interests and involve potential adversaries with suspected or known CNA capability. - Military ops, contingency, or exercise planned or ongoing requiring increased security of information systems. - Information system probes, scans or other activities detected.	- Accomplish all actions required at INFOCON NORMAL - Execute appropriate security practices. For example: -- Increase level of auditing, review, and file back-up procedures. -- Conduct internal security review on critical systems. -- Heighten awareness of all info systems users. -- Execute appropriate defensive

INFOCON Level: BRAVO
Specific Risk of Attack

CRITERIA	RECOMMENDED ACTIONS
- Indications & Warning (I&W) indicate targeting of specific system, location, unit, or operation. - Major military ops, contingency, or exercise planned or ongoing requiring increased security of information systems. *- Significant level of network probes, scans or other activities detected.* *- Network penetration or denial of service attempted with no impact to DoD operations.*	- Accomplish all actions required at INFOCON ALPHA. - Execute appropriate security practices. For example: -- Increase level of auditing, review, and file back-up procedures. *-- Conduct immediate internal security review on critical systems.* -- Heighten awareness of all info systems users. -- Execute appropriate defensive

INFOCON Level: CHARLIE
Limited Attack(s)

CRITERIA	RECOMMENDED ACTIONS
- Intelligence attack assessment(s) indicate a limited attack. ***- Information system attack(s) detected with limited impact to DoD operations:*** -- Minimal success, successfully counteracted. -- Little or no data or systems compromised. -- Unit able to accomplish mission.	- Accomplish all actions required at INFOCON BRAVO. - Execute appropriate response actions. For example: -- Maximum level of auditing, review, and file back-up procedures. ***-- Limit traffic to mission essential communication only.*** ***-- Reroute mission-critical communication through unaffected systems.*** ***-- Disconnect non-mission-critical networks.*** -- Execute appropriate defensive

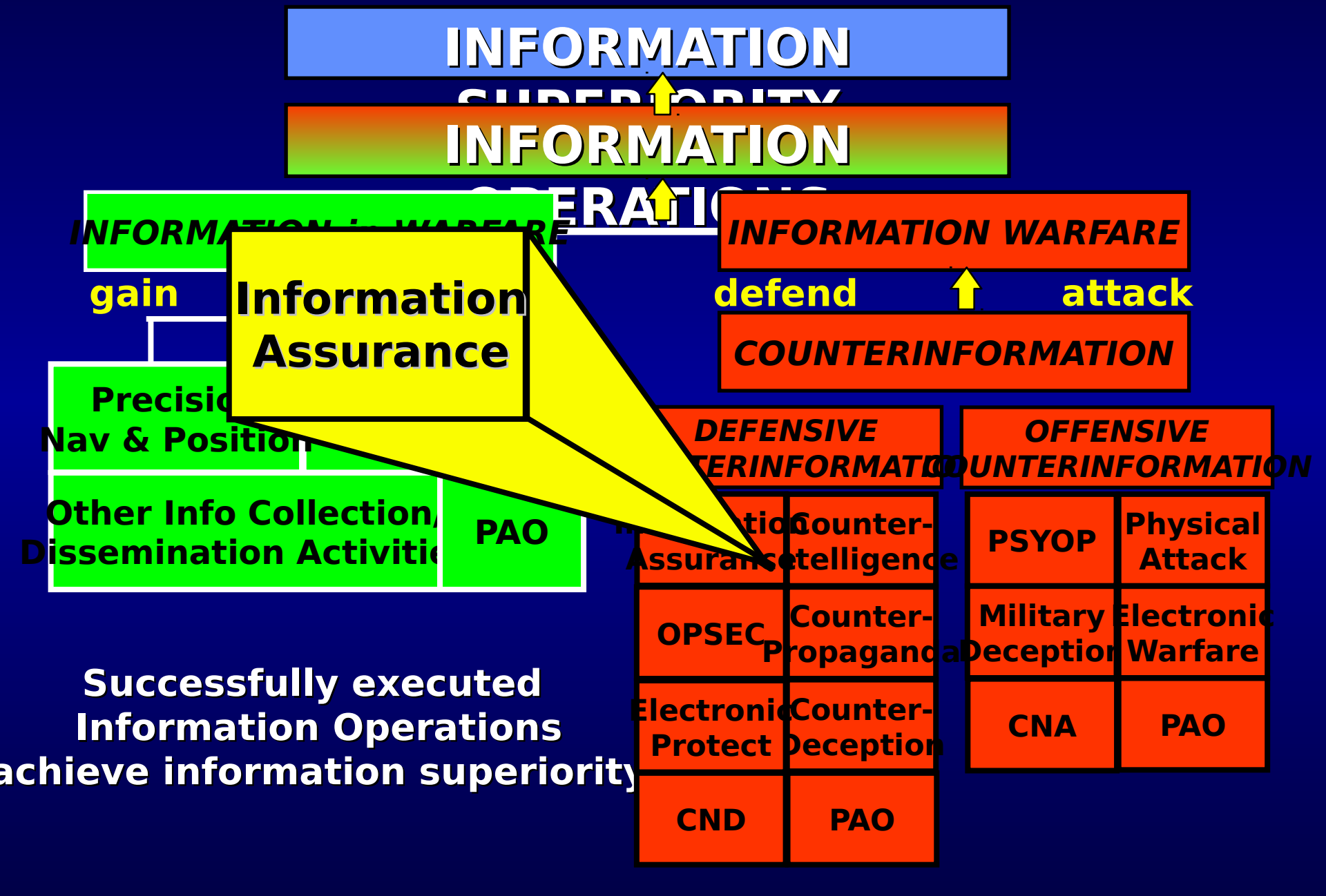
INFOCON Level: DELTA
General Attack(s)

CRITERIA	RECOMMENDED ACTIONS
- Intelligence attack assessment(s) indicate a limited attack. *- Successful information system attack(s) detected which impact to DoD operations:* *-- Widespread incidents that undermine ability to function effectively.* *-- Significant risk of mission failure.*	- Accomplish all actions required at INFOCON CHARLIE. - Execute appropriate response actions. For example: *-- Designate alternate information systems* *-- Implement procedures for conducting operations in "stand-alone" mode or manually.* *-- Isolate compromised systems from rest of network.*

INFOCON Impact

	Gain	Loss
Normal	• **Full Connectivity** • **No bandwidth restrictions** • **Normal OPTEMPO**	• **Normal defensive posture; no additional measures taken**
Alpha	• **10% improved protection** • Increased likelihood intruders will be defeated or caught • If sufficient, no need for higher INFOCON	• **0% reduction in OPTEMPO** • **0% reduced connectivity** • Affected networks may be isolated • **0% delay in information access**
Bravo	• **35% improved protection** • Increased likelihood intruders will be defeated or caught • If sufficient, no need for higher INFOCON	• **25% reduction in OPTEMPO** • **20% reduction in connectivity** • Affected networks may be isolated
Charlie	• **75% improved protection** • Increased likelihood intruders will be defeated or caught • If sufficient, no need for higher INFOCON	• **50% reduction in OPTEMPO** • **40% reduction in connectivity** • Affected networks may be isolated
Delta	• **90% improved protection** • Increased likelihood intruders will be defeated or caught • If sufficient, no need for higher	• **70% reduction in OPTEMPO** • **60% reduction in connectivity** • Affected networks may be isolated

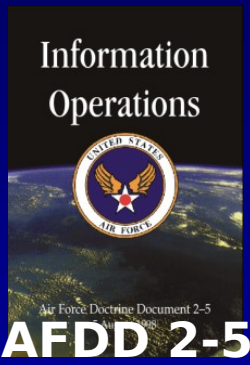
AFDD 2-5



Successfully executed Information Operations achieve information superiority


COMSEC
COMPUSEC
EMSEC
IAAP
Information Assurance

Information Assurance



AFDD 2-5

… those measures to protect and defend information and information systems by ensuring their *availability, integrity, authenticity, confidentiality*, and *non-repudiation.*

Availability **- resources are available when needed**

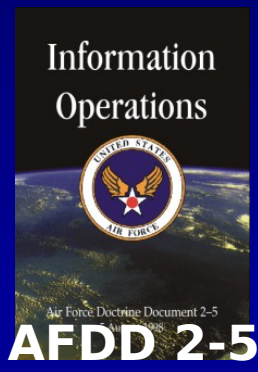
Integrity **- resources operate correctly**

Authenticity **- ensures information is trustworthy (fact or actuality)**

Confidentiality **- only those with proper clearance and need- to-know have access to sensitive information**

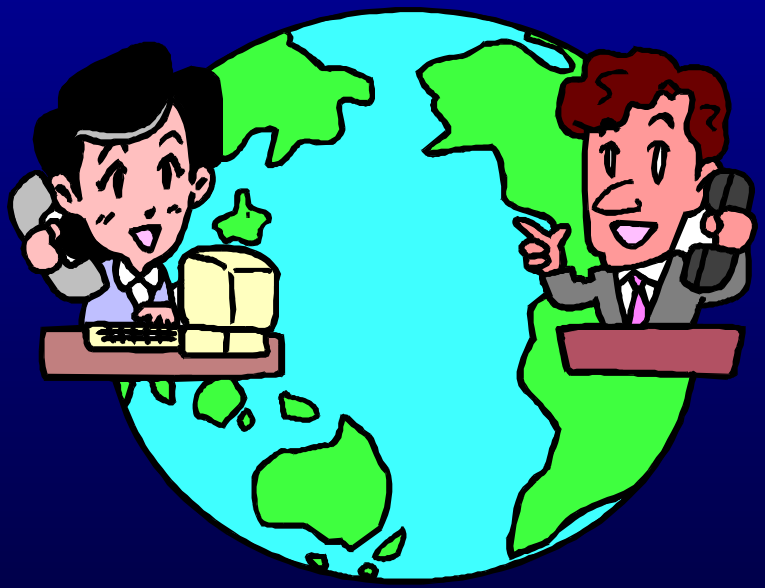
Non-repudiation **- ability to confirm source of transmission and data**

Communications Security (COMSEC)



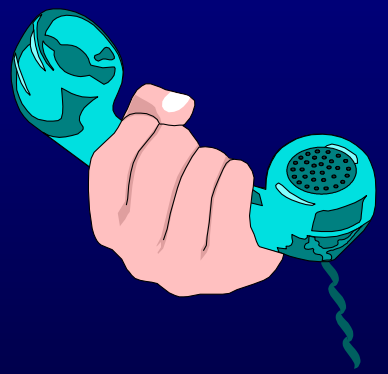
AFDD 2-5

... measures and controls taken to deny unauthorized persons information derived from telecommunications while also ensuring telecommunications authenticity.

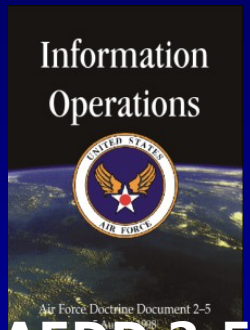


Emissions Security (EMSEC)

“Protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment, information systems, and telecommunications systems.”

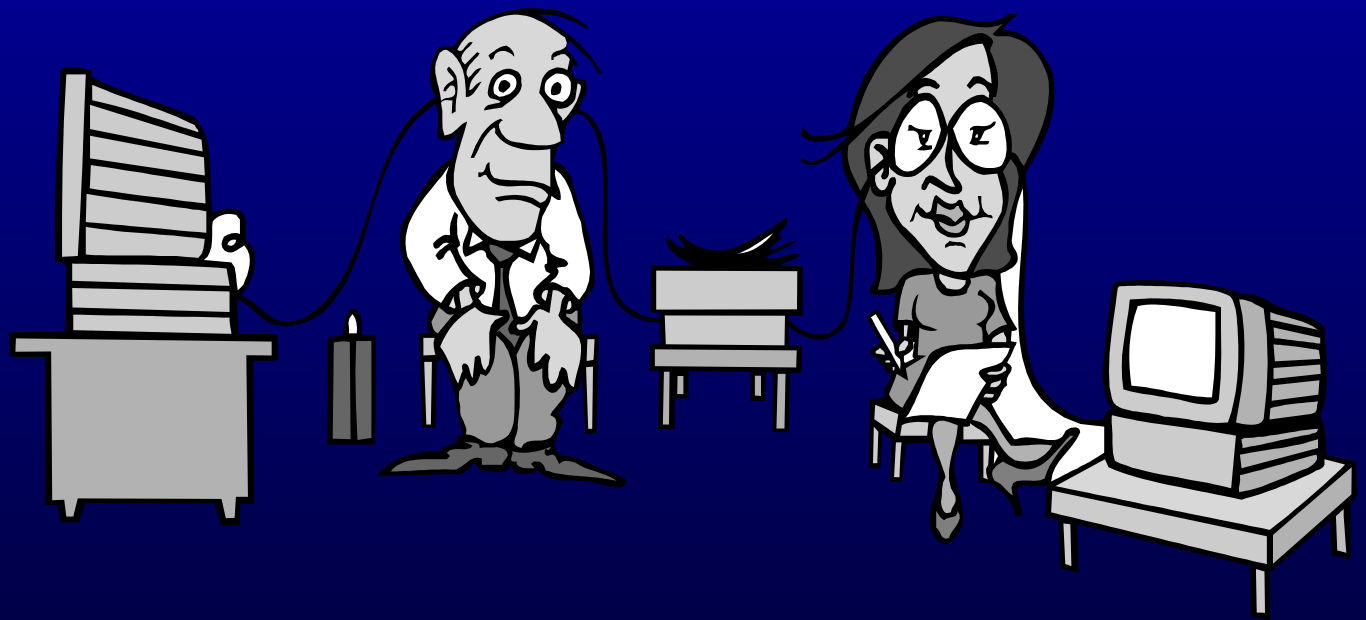


Computer Security (COMPUSEC)



AFDD 2-5

… measures and controls that ensure the confidentiality, integrity, or availability of information processed and stored by a computer.



Why all the hype?

"DoD Escalates War Against Poor Computer Security."

"Insiders account for more security compromises than hackers."

"Weak passwords allow easy access for unauthorized personnel."

"The disgruntled employee is our primary concern, not competition."

COMPUSEC


THREATS
VULNERABILITES
RISK MANAGEMENT
COUNTERMEASURES
RISKS

COMPUSEC

- Natural
- Environmental
- Human

Natural Threats

- Earthquake
- Flood
- Hurricane
- Snow/Ice
- Tornado
- Lightning
- Severe Storm

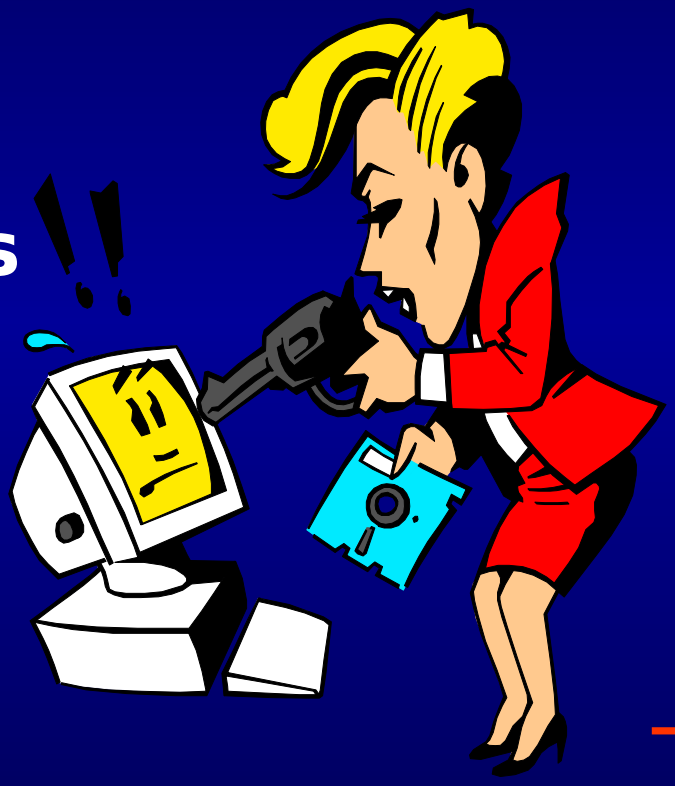
Environmental Threats

- Power Disruption
- Utility Failure
- Smoke
- Water
- Fire

→ Hardware Failure
→ Software Failure
→ Personnel Injury
→ Explosion

Human Threats
Intentional

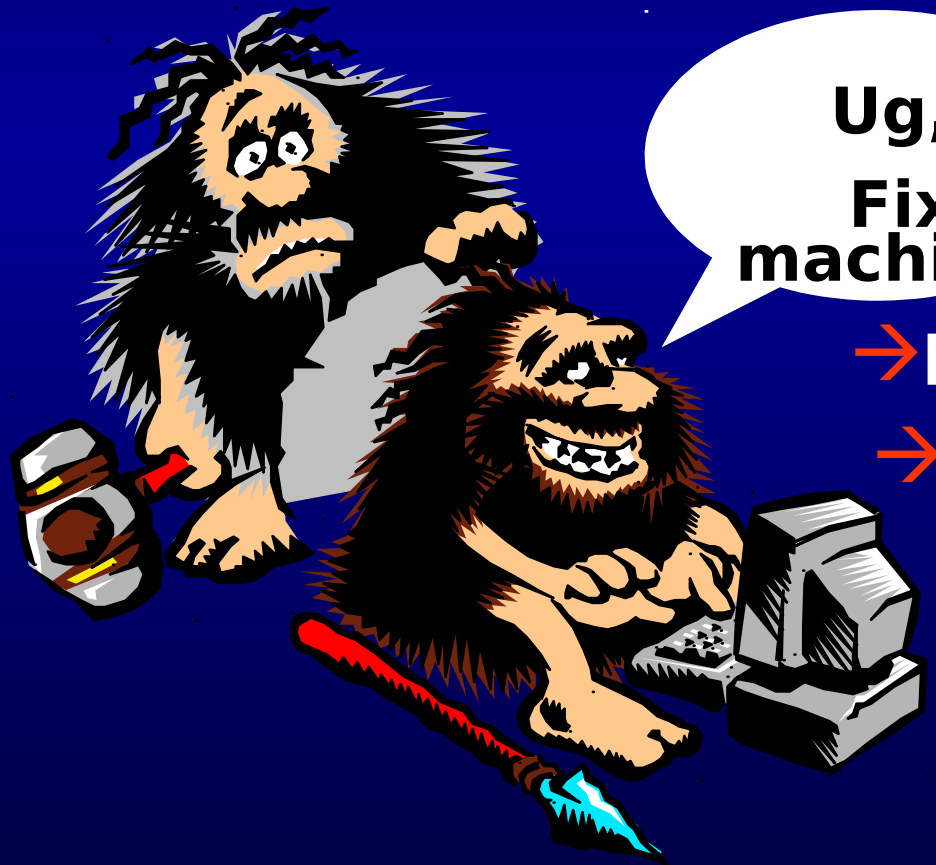
- Bomb Threat
- Compromise
- Disclosure
- Sabotage
- Misuse



→Theft
→Fraud
→Viruses
→Alteration
→Destruction
→Unauthorized Access

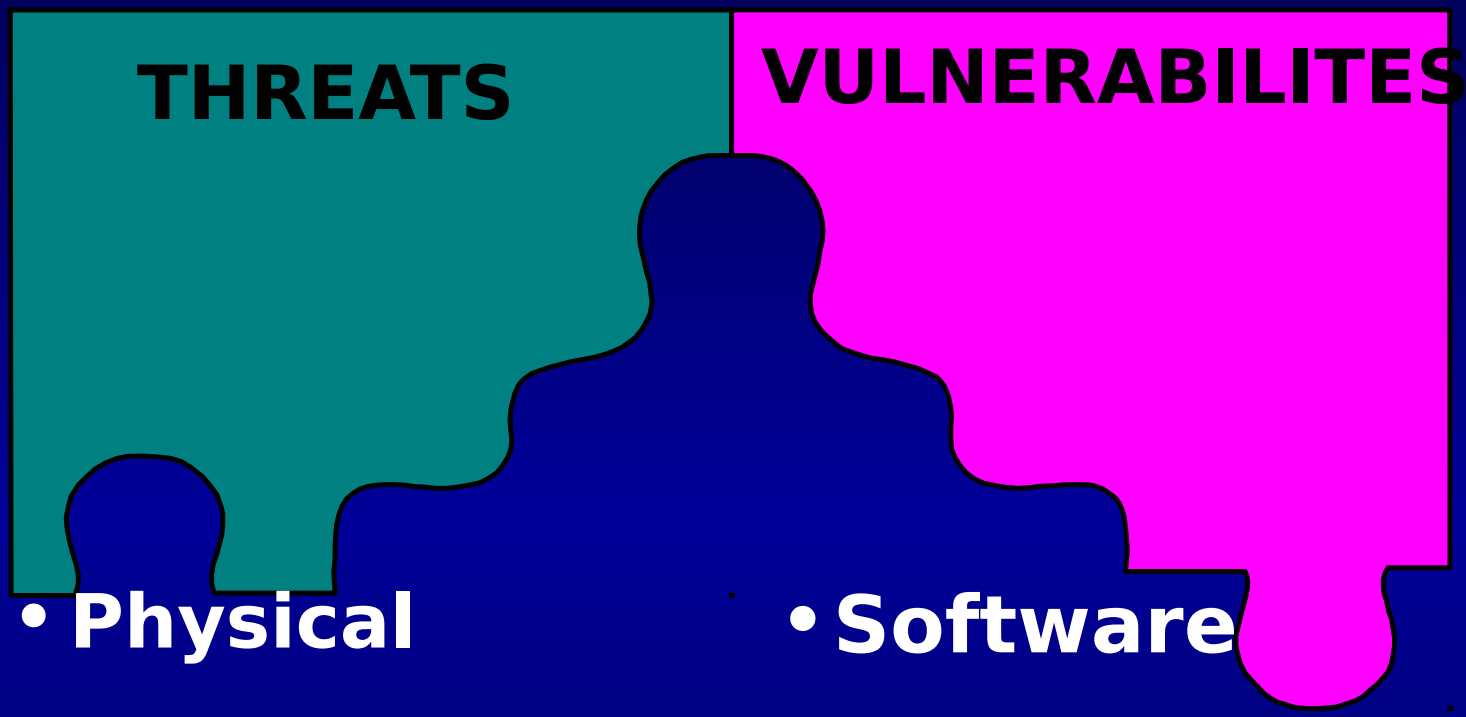
Human Threats
Unintentional

- Deficiency in Policy or Procedure
- General Errors
- Data Loss



→ Hardware Failure
→ Software Failure
→ Comm Failure
→ Compromise
→ Disclosure

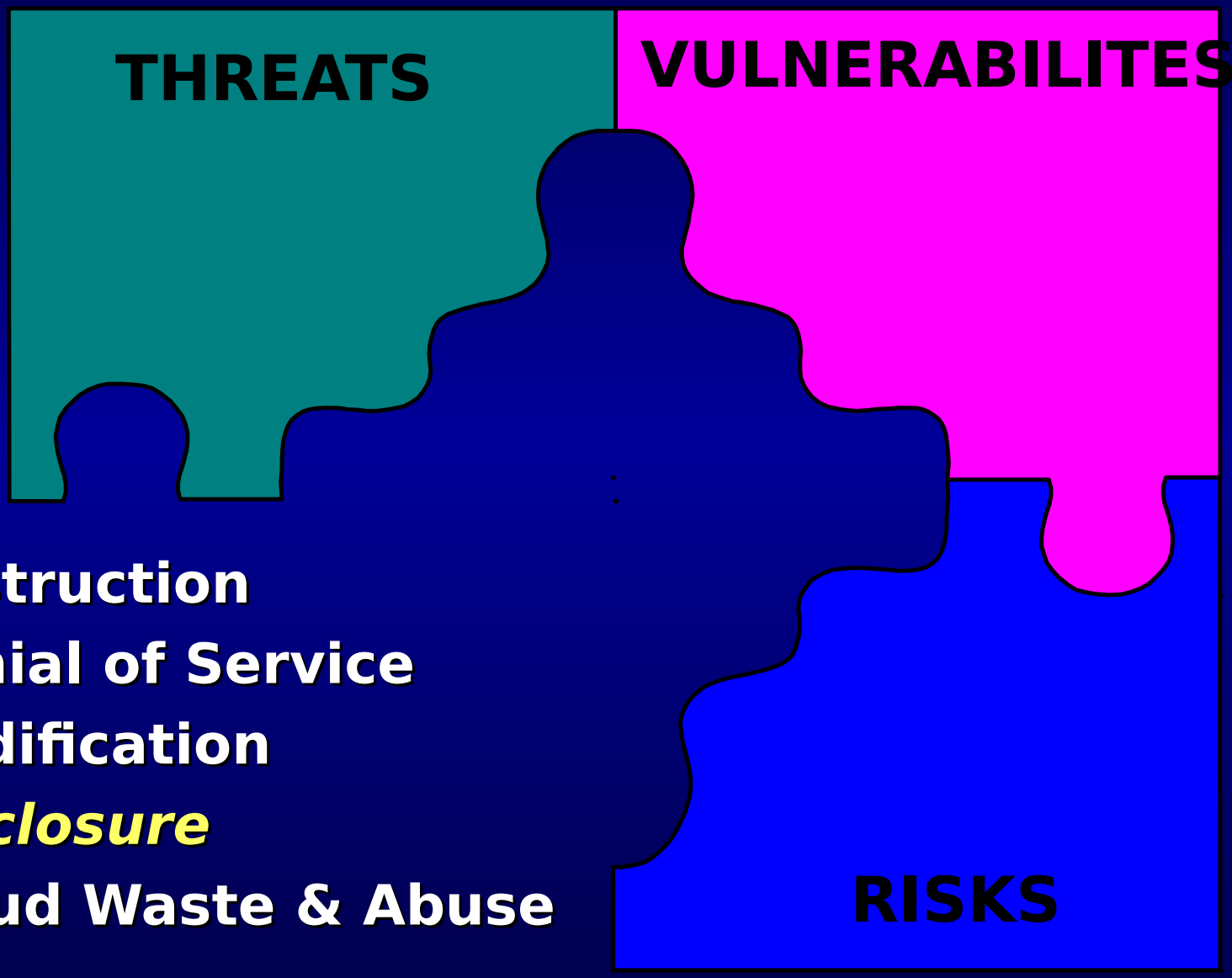
COMPUSEC



- Physical
- Environmental
- Personnel
- Hardware

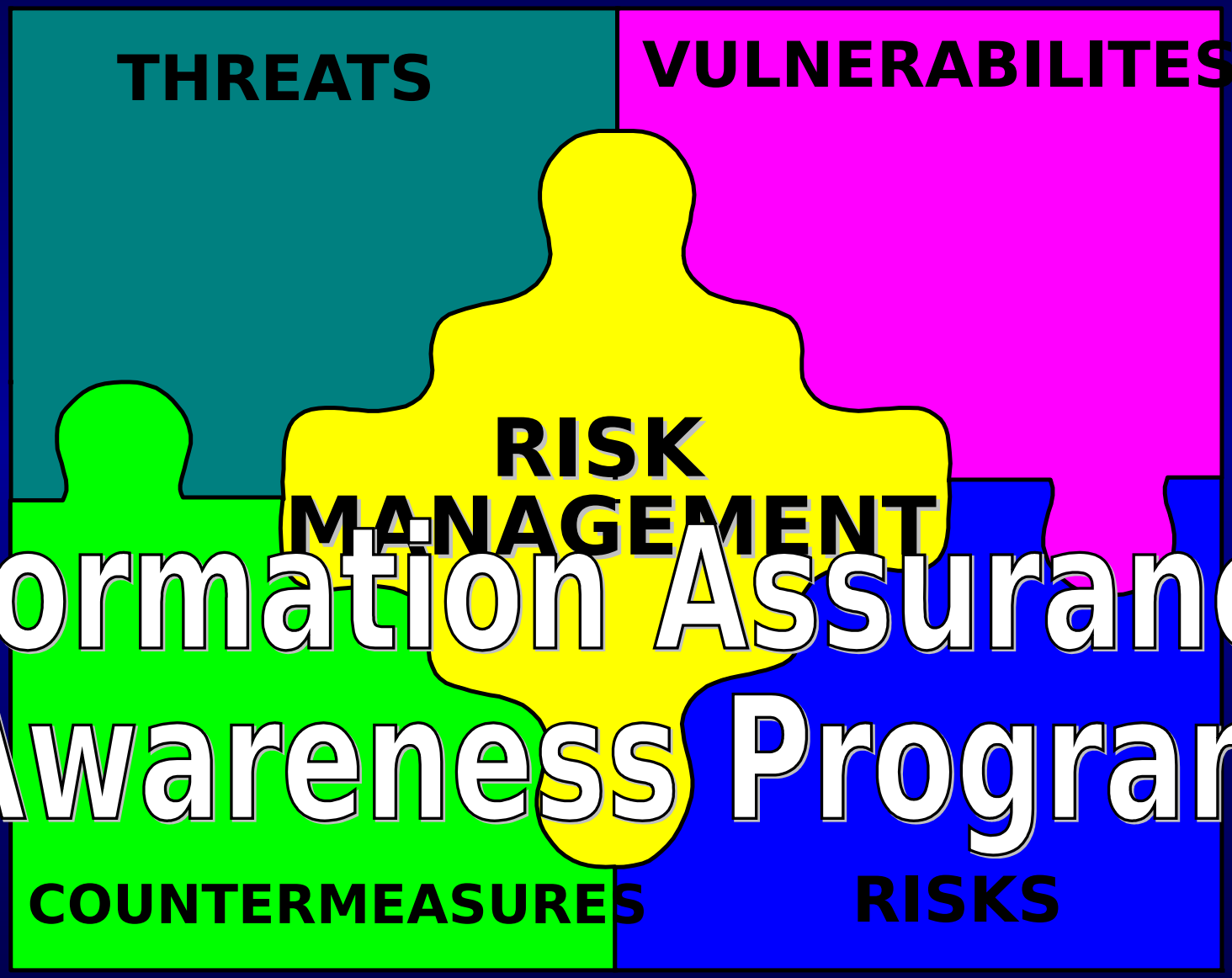
- Software
- Media
- Network
- Procedural

COMPUSEC



- Destruction
- Denial of Service
- Modification
- *Disclosure*
- Fraud Waste & Abuse

COMPUSEC



Information Assurance Awareness Program

First Report Card on Computer Security

- Federal Departments and Agencies
- Prepared for the Subcommittee on Gov't Management, Information, & Technology
- 11 Sep 2000
- Conducted by the GAO and agency Inspectors General
- First-time such government-wide information has ever been compiled

COMPUSEC Report Card

Dept/Agency	00	01	02
Social Security Admin	B	C+	B-
Nat'l Science Foundation	B-	B+	D-
Education	C	F	D
State	C	D+	F
Housing & Urban Dev't	C-	D+	F
Commerce	C-	F	D+
Agency Intern'l Dev't	C-	F	F
Defense	D+	F	F
Veterans Affairs	D	F	F
Treasury	D	F	F
Envir't Protection Agency	D-	D+	D-
General Services	D-	D+	D

Dept/Agency	00	01	02
NASA	D-	C-	D+
Office of Person'l Mgmt	F	F	F
Health & Human Services	F	F	D-
Agriculture	F	F	F
Small Business Admin	F	F	F
Justice	F	F	F
Labor	F	F	C+
Interior	IC	F	F
Energy	IC	F	F
Nuclear Regulatory Com	IC	F	F
Transportation	IC	D	F

GOV'T WIDE GRADE D- F

Stay Current

How / Who do you report problems / issues?

- **Workgroup Manager / ISSO**
- **Unit COMPUSEC Manager (UCM)**
- **Base COMPUSEC Manager @ WIPO**

AF Publications on Communication & Information (33 Series):
http://afpubs.hq.af.mil

“The top information warfare priority is to **defend our own** increasingly information intensive capabilities.”

OPSEC COMSEC CND YOU EMSEC COMPUSEC

IDENTIFY AND ELIMINATE YOUR WEAK LINK!